日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　５月１０日

出願番号
Application Number: 特願２０００－１４２３０７

出願人
Applicant(s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　５月３０日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０４７３４４

【書類名】　特許願
【整理番号】　0000440503
【提出日】　平成12年 5月10日
【あて先】　特許庁長官殿
【国際特許分類】　H04K　1/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　大嶋　拓哉
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
　【代表者】　出井　伸之
【代理人】
　【識別番号】　100094053
　【弁理士】
　【氏名又は名称】　佐藤　隆久
【手数料の表示】
　【予納台帳番号】　014890
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9707389
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信システム、通信装置および通信方法

【特許請求の範囲】

【請求項１】

通信装置、サービス提供装置および管理装置を有し、前記サービス提供装置が提供するサービスあるいは商品に関する支払い処理をＩＣカードを用いて行う通信システムであって、

前記管理装置は、前記ＩＣカード内で支払い処理を行うための支払い処理情報を前記サービス提供装置からの支払い請求情報に基づいて生成し、当該支払い処理情報を当該管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し、当該暗号化した支払い処理情報と当該管理装置の署名情報とを前記通信装置に送信し、

前記通信装置は、前記管理装置から受信した前記署名情報の正当性を検証した後に、前記支払い処理情報を前記ＩＣカードに出力する

通信システム。

【請求項２】

前記管理装置は、当該管理装置の秘密鍵を用いて前記署名情報を作成し、

前記通信装置は、前記秘密鍵に対応する公開鍵を用いて前記署名情報の正当性を検証する

請求項１に記載の通信システム。

【請求項３】

前記サービス提供装置は、支払い請求情報の正当性を示す署名情報を当該サービス提供装置の秘密鍵を用いて作成し、当該署名情報が付された前記支払い請求情報を、前記通信装置を介して前記管理装置に送信し、

前記管理装置は、前記サービス提供装置が作成した前記署名情報の正当性を前記サービス提供装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記支払い処理情報と前記管理装置の前記署名情報とを前記通信装置に送信する

請求項１に記載の通信システム。

【請求項４】

前記通信装置は、前記支払い請求情報の内容の表示あるいは音声出力を行い、当該内容に同意したことを示す指示をユーザから受けた後に、前記暗号化された前記支払い処理情報を前記ＩＣカードに出力する

請求項１に記載の通信システム。

【請求項５】

前記管理装置は、前記共通鍵を用いて作成した前記ＩＣカードの残高情報読み出し要求を前記通信装置に送信し、前記ＩＣカードから読み出された残高情報を前記通信装置から受信し、当該残高情報を前記共通鍵を用いて復号し、

前記通信装置は、前記管理装置からの前記残高情報読み出し要求を前記ＩＣカードに送信し、前記ＩＣカードからの前記残高情報を前記管理装置に送信する

請求項１に記載の通信システム。

【請求項６】

前記管理装置は、前記復号した残高情報を前記共通鍵で暗号化しないで前記支払い処理情報と共に前記通信装置に送信し、

前記通信装置は、前記管理装置から受信した前記残高情報が示す金額を表示あるいは音声出力し、当該金額に同意したことを示す指示をユーザから受けた後に、前記管理装置から受信した前記支払い処理情報を前記ＩＣカードに出力する

請求項５に記載の通信システム。

【請求項７】

前記支払い処理情報は、前記ＩＣカード内で、当該ＩＣカードに記憶されている前記残高情報が示す金額から、前記支払い請求情報が示す金額を減算し、当該減算の結果を示す前記残高情報を前記ＩＣカードに記憶するための情報である

請求項１に記載の通信システム。

【請求項８】

前記管理装置は、前記サービス提供装置が作成した前記支払い請求情報に基づいて、前記支払い処理に関しての所定の履歴情報を作成し、当該履歴情報を前記共通鍵で暗号化して前記支払い処理情報と共に前記通信装置に送信し、

前記通信装置は、前記管理装置から受信した前記履歴情報を前記ＩＣカードに

出力する

請求項１に記載の通信システム。

【請求項９】

前記通信装置は、前記支払い処理情報に応じた支払い処理が適切に行われたことを示す通知を前記ＩＣカードから入力すると、当該通知を前記管理装置に送信する

請求項１に記載の通信システム。

【請求項１０】

前記管理装置は、前記通信装置から前記通知を受信すると、支払いが完了したことを示す支払い完了通知を前記通信装置および前記サービス提供装置に送信する

請求項９に記載の通信システム。

【請求項１１】

前記通信装置は、前記ＩＣカードにアクセス可能なアクセス装置との間で、前記支払い処理情報の出力、並びに所定の情報の入出力を行う

請求項１に記載の通信システム。

【請求項１２】

前記通信装置は、ブラウザプログラムを実行して前記サービス提供装置との間で通信を行い、当該ブラウザプログラムを実行中に、所定のインターフェースプログラムを実行して前記アクセス装置を介して前記ＩＣカードとの間で情報の入出力を行う

請求項１１に記載の通信システム。

【請求項１３】

前記サービス提供装置は、前記支払い請求情報と共に前記インターフェースプログラムを前記通信装置に送信する

請求項１１に記載の通信システム。

【請求項１４】

前記通信装置は、前記サービス提供装置との間で、当該サービス提供装置が提供するサービスあるいは商品を受けるための所定の情報の送受信を行う

請求項１に記載の通信システム。

【請求項１５】

前記サービス提供装置は、

前記サービスあるいは商品に関しての支払い手続を行う旨の指示を前記通信装置から受けると、当該サービスあるいは商品についての前記支払い請求情報を前記通信装置に送信し、

前記通信装置は、前記サービス提供装置から受信した支払い請求情報の内容を表示あるいは出力し、当該内容に同意したことを示す指示をユーザから受けた後に、前記支払い請求情報を前記管理装置に送信する

請求項１４に記載の通信システム。

【請求項１６】

前記管理装置は、

前記共通鍵を保持し、前記支払い処理情報の生成、並びに前記共通鍵を用いた暗号化を行う第１の管理装置と、

前記第１の管理装置から入力した前記暗号化された前記支払い処理情報について当該管理装置の秘密鍵を用いて前記署名情報を作成し、前記暗号化された支払い処理情報と前記署名情報とを前記通信装置に送信する第２の管理装置と

を有する

請求項１に記載の通信システム。

【請求項１７】

前記通信装置および前記管理装置は、

前記通信装置と前記管理装置との間で情報または要求を送受信する際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において当該秘密鍵に対応する公開鍵を用いて検証する

請求項１に記載の通信システム。

【請求項１８】

前記通信装置および前記サービス提供装置は、

前記通信装置と前記サービス提供装置との間で情報または要求を送受信する際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において当該秘密鍵に

対応する公開鍵を用いて検証する

請求項１に記載の通信システム。

【請求項１９】

前記通信装置、前記サービス提供装置および前記管理装置は、ネットワークを介して前記情報の送受信を行う

請求項１に記載の通信システム。

【請求項２０】

サービス提供装置が提供するサービスあるいは商品に対しての支払い処理をＩＣカードを用いて行う場合に、当該ＩＣカードとの間で情報の入出力を行う他の通信装置との間で通信を行う通信装置であって、

前記ＩＣカード内で支払い処理を行うための支払い処理情報を当該通信装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し、当該暗号化した支払い処理情報の正当性を示す当該通信装置の署名情報を生成し、前記暗号化した支払い処理情報と前記署名情報とを前記他の通信装置に送信する

通信装置。

【請求項２１】

当該通信装置の秘密鍵を用いて前記署名情報を作成する

請求項２０に記載の通信装置。

【請求項２２】

前記サービス提供装置が作成した署名情報の正当性を、前記サービス提供装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記支払い処理情報と前記管理装置の前記署名情報とを前記他の通信装置に送信する

請求項２０に記載の通信装置。

【請求項２３】

前記共通鍵を保持し、前記支払い処理情報の生成、並びに前記共通鍵を用いた前記支払い処理情報の暗号化を行う第１の管理装置と、

前記第１の管理装置から入力した前記暗号化された前記支払い処理情報について当該通信装置の秘密鍵を用いて前記署名情報を作成し、前記暗号化された支払い処理情報と前記署名情報とを前記他の通信装置に送信する第２の管理装置と

を有する

請求項２０に記載の通信装置。

【請求項２４】

通信装置、サービス提供装置および管理装置を用いて、前記サービス提供装置が提供したあるいは提供するサービスあるいは商品に対しての支払い処理をＩＣカードを用いて行う通信方法であって、

前記管理装置において、前記ＩＣカード内で支払い処理を行うための支払い処理情報を前記サービス提供装置からの支払い請求情報に基づいて生成し、当該支払い処理情報を当該管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し、

当該暗号化した支払い処理情報と当該管理装置の署名情報とを前記管理装置から前記通信装置に送信し、

前記通信装置において、前記管理装置から受信した前記署名情報の正当性を検証した後に、前記支払い処理情報を前記ＩＣカードに出力する

通信方法。

【請求項２５】

前記管理装置において、当該管理装置の秘密鍵を用いて前記署名情報を作成し、

前記通信装置において、前記秘密鍵に対応する公開鍵を用いて前記署名情報の正当性を検証する

請求項２４に記載の通信方法。

【請求項２６】

前記サービス提供装置において、支払い請求情報の正当性を示す署名情報を当該サービス提供装置の秘密鍵を用いて作成し、

当該署名情報が付された前記支払い請求情報を、前記通信装置を介して前記サービス提供装置から前記管理装置に送信し、

前記管理装置において、前記サービス提供装置が作成した前記署名情報の正当性を前記サービス提供装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記支払い処理情報と前記管理装置の前記署名情報とを前記通信装置に送信する

請求項２４に記載の通信方法。

【請求項２７】

前記通信装置において、前記支払い請求情報の内容の表示あるいは音声出力を行い、当該内容に同意したことを示す指示をユーザから受けた後に、前記暗号化された前記支払い処理情報を前記ＩＣカードに出力する

請求項２４に記載の通信方法。

【請求項２８】

前記共通鍵を用いて作成した前記ＩＣカードの残高情報読み出し要求を前記管理装置から前記通信装置に送信し、

前記通信装置において、前記管理装置からの前記残高情報読み出し要求を前記ＩＣカードに出力し、

前記ＩＣカードにおいて、前記通信装置から入力した前記残高情報読み出し要求に応じて、当該ＩＣカード内の記憶回路から残高情報を読み出し、当該読み出した残高情報を通信装置を介して前記管理装置に送信し、

前記管理装置において、前記通信装置から受信した残高情報を前記共通鍵を用いて復号する

請求項２４に記載の通信方法。

【請求項２９】

前記管理装置から前記通信装置に、前記復号した残高情報を前記共通鍵で暗号化しないで前記支払い処理情報と共に送信し、

前記通信装置において、前記管理装置から受信した前記残高情報が示す金額を表示あるいは音声出力し、当該金額に同意したことを示す指示をユーザから受けた後に、前記管理装置から受信した前記支払い処理情報を前記ＩＣカードに出力する

請求項２４に記載の通信方法。

【請求項３０】

前記支払い処理情報は、前記ＩＣカード内で、当該ＩＣカードに記憶されている前記残高情報が示す金額から、前記支払い請求情報が示す金額を減算し、当該減算の結果を示す前記残高情報を記憶するための情報である

請求項２４に記載の通信方法。

【請求項３１】

前記管理装置において、前記サービス提供装置が作成した前記支払い請求情報に基づいて、前記支払い処理に関しての所定の履歴情報を作成し、当該履歴情報を前記共通鍵で暗号化し、

当該暗号化した前記履歴情報を前記支払い処理情報と共に前記管理装置から前記通信装置に送信し、

前記通信装置において、前記管理装置から受信した前記残高情報が示す金額に同意したことを示す指示をユーザから受けた後に、前記管理装置から受信した前記履歴情報を前記ＩＣカードに出力し、

前記ＩＣカードは、前記通信装置から入力した前記履歴情報を記憶する

請求項２４に記載の通信方法。

【請求項３２】

前記通信装置は、前記ＩＣカードにアクセス可能なアクセス装置との間で、前記支払い処理情報の出力、並びに所定の情報の入出力を行う

請求項２４に記載の通信方法。

【請求項３３】

前記ＩＣカードは、耐タンパ性のモジュール内で、前記支払い処理情報に応じた前記支払い処理を行う

請求項２４に記載の通信方法。

【請求項３４】

前記通信装置と前記管理装置との間で情報または要求を送受信する際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において当該秘密鍵に対応する公開鍵を用いて検証する

請求項２４に記載の通信方法。

【請求項３５】

前記通信装置および前記サービス提供装置は、

前記通信装置と前記サービス提供装置との間で情報または要求を送受信する際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において当該秘密鍵に

対応する公開鍵を用いて検証する

請求項２４に記載の通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、共通鍵を保持したＩＣカードを用いて、ネットワークなどを用いた決済処理を安全に行うことができる通信システム、通信装置および通信方法に関する。

【０００２】

【従来の技術】

ネットワークを介した電子商取引を安全に行うために、通常、ＰＫＩ(Public Key Infrastructure：公開鍵インフラ）プロトコルが採用されている。

ＰＫＩプロトコルでは、送信元で秘密鍵を用いて署名情報を作成し、送信先から送信先に、当該署名情報を伝送情報と共に送信する。そして、送信先において、当該秘密鍵に対応する公開鍵を用いて当該署名情報の検証を行うことで、受信した伝送情報が正当な送信元で作成されたものであるか否かを判断する。

【０００３】

ところで、近年、ＩＣ(Integrated Circuit)カードを用いて、ネットワークを介した電子商取引を行う試みがある。

ここで、通常、ＩＣカードは、共通鍵を保持しており、共通鍵暗号方式を用いて秘匿性のある情報の入出力を行う。このようなＩＣカードは、共通鍵が署名情報を作成するための鍵とはなり得ないため、ＩＣカードを紛失した場合でも、被害を小さくできるという利点がある。

【０００４】

【発明の解決しようとする課題】

しかしながら、ネットワークを介した電子商取引を安全に行うためには、秘密鍵を用いて署名情報を作成する必要があるが、従来の手法では、ＩＣカードが秘密鍵を保持（記憶）していないため、署名情報の作成ができないという問題がある。

この場合に、ＩＣカードに秘密鍵を保持する方法も考えられるが、前述したように、秘密鍵は署名情報を作成できるため印鑑照明と同様の効力があり、ＩＣカードを紛失して悪用されたときの被害が大きすぎるという問題がある。

また、上述したようなＩＣカードが採用する共通鍵暗号方式のみを用いて、ネットワークを介した電子商取引を行うと、取り引きを行う多数の相手先のサーバ装置などが共通鍵を持つことになり、共通鍵が盗まれたり、悪用される可能性が高くなるという問題もある。

【０００５】

本発明は上述した従来技術の問題点に鑑みてなされ、共通鍵を保持したＩＣカードを用いて、ネットワークを介した電子商取引を安全に行うことができる通信システム、通信装置および通信方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第１の発明の通信システムは、通信装置、サービス提供装置および管理装置を有し、前記サービス提供装置が提供するサービスあるいは商品に関する支払い処理をＩＣカードを用いて行う通信システムであって、前記管理装置は、前記ＩＣカード内で支払い処理を行うための支払い処理情報を前記サービス提供装置からの支払い請求情報に基づいて生成し、当該支払い処理情報を当該管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し、当該暗号化した支払い処理情報と当該管理装置の署名情報とを前記通信装置に送信し、前記通信装置は、前記管理装置から受信した前記署名情報の正当性を検証した後に、前記支払い処理情報を前記ＩＣカードに出力する。

【０００７】

第１の発明の通信システムの作用は以下のようになる。

サービス提供装置において、サービスあるいは商品を提供したことに関する情報が生成され、当該情報が管理装置に送信される。

次に、管理装置は、前記ＩＣカード内で支払い処理を行うための支払い処理情報を前記サービス提供装置からの支払い請求情報に基づいて生成し、当該支払い

処理情報を当該管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し、当該暗号化した支払い処理情報と当該管理装置の署名情報とを前記通信装置に送信する。

次に、前記通信装置は、前記管理装置から受信した前記署名情報の正当性を検証した後に、前記支払い処理情報を前記ＩＣカードに出力する。

第１の発明の通信システムでは、支払い処理情報は、前記管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化されているため、安全性が保たれる。すなわち、当該共通鍵は、前記管理装置と前記ＩＣカードとの間でのみ共用され、それ以外の装置には供給されないため、共通鍵の管理が容易であると共に、共通鍵を不正に取得される可能性を低くできる。また、共通鍵をＩＣカード内の耐タンパ性のメモリに記憶し、ＩＣカードの外部に読み出しできないようにすることで、ＩＣカードのユーザであっても、当該共通鍵を用いて支払い処理情報を不正に改竄できない。

また、第１の発明の通信システムでは、支払い処理情報に管理装置の署名情報を付して通信装置に送信し、通信装置において、受信した署名情報を検証することで、支払い処理情報が通信経路上で不正に改竄されたか否かを通信装置で検証でき、通信経路上での安全性を保証できる。

【０００８】

また、第１の発明の通信システムは、好ましくは、前記管理装置は、当該管理装置の秘密鍵を用いて前記署名情報を作成し、前記通信装置は、前記秘密鍵に対応する公開鍵を用いて前記署名情報の正当性を検証する。

【０００９】

また、第１の発明の通信システムは、好ましくは、前記サービス提供装置は、前記支払い請求情報の正当性を示す署名情報を当該サービス提供装置の秘密鍵を用いて作成し、当該署名情報が付された前記支払い請求情報を、前記通信装置を介して前記管理装置に送信し、前記管理装置は、前記サービス提供装置が作成した前記署名情報の正当性を、前記サービス提供装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記支払い処理情報と前記管理装置の前記署名情報とを前記通信装置に送信する。

【００１０】

また、第１の発明の通信システムは、好ましくは、前記通信装置は、前記支払い請求情報の内容の表示あるいは音声出力を行い、当該内容に同意したことを示す指示をユーザから受けた後に、前記暗号化された前記支払い処理情報を前記ＩＣカードに出力する。

【００１１】

また、第１の発明の通信システムは、好ましくは、前記管理装置は、前記共通鍵を用いて作成した前記ＩＣカードの残高情報読み出し要求を前記通信装置に送信し、前記ＩＣカードから読み出された残高情報を前記通信装置から受信し、当該残高情報を前記共通鍵を用いて復号し、前記通信装置は、前記管理装置からの前記残高情報読み出し要求を前記ＩＣカードに送信し、前記ＩＣカードからの前記残高情報を前記管理装置に送信する。

【００１２】

また、第１の発明の通信システムは、好ましくは、前記管理装置は、前記復号した残高情報を前記共通鍵で暗号化しないで前記支払い処理情報と共に前記通信装置に送信し、前記通信装置は、前記管理装置から受信した前記残高情報が示す金額を表示あるいは音声出力し、当該金額に同意したことを示す指示をユーザから受けた後に、前記管理装置から受信した前記支払い処理情報を前記ＩＣカードに出力する。

【００１３】

また、第１の発明の通信システムは、好ましくは、前記支払い処理情報は、前記ＩＣカード内で、当該ＩＣカードに記憶されている前記残高情報が示す金額から、前記支払い請求情報が示す金額を減算し、当該減算の結果を示す前記残高情報を記憶するための情報である。

【００１４】

また、第１の発明の通信システムは、好ましくは、前記管理装置は、前記サービス提供装置が作成した前記支払い請求情報に基づいて、前記支払い処理に関しての所定の履歴情報を作成し、当該履歴情報を前記共通鍵で暗号化して前記支払い処理情報と共に前記通信装置に送信し、前記通信装置は、前記管理装置から受

信した前記履歴情報を前記ＩＣカードに出力する。

【００１５】

また、第１の発明の通信システムは、好ましくは、前記通信装置は、前記支払い処理情報に応じた支払い処理が適切に行われたことを示す通知を前記ＩＣカードから入力すると、当該通知を前記管理装置に送信する。

【００１６】

また、第１の発明の通信システムは、好ましくは、前記管理装置は、前記通信装置から前記通知を受信すると、支払いが完了したことを示す支払い完了通知を前記通信装置および前記サービス提供装置に送信する。

【００１７】

また、第１の発明の通信システムは、好ましくは、前記通信装置は、前記ＩＣカードにアクセス可能なアクセス装置との間で、前記支払い処理情報の出力、並びに所定の情報の入出力を行う。

【００１８】

また、第１の発明の通信システムは、好ましくは、前記通信装置は、ブラウザプログラムを実行して前記サービス提供装置との間で通信を行い、当該ブラウザプログラムを実行中に、所定のインターフェースプログラムを実行して前記アクセス装置を介して前記ＩＣカードとの間で情報の入出力を行う。

【００１９】

また、第１の発明の通信システムは、好ましくは、前記サービス提供装置は、前記支払い請求情報と共に前記インターフェースプログラムを前記通信装置に送信する。

【００２０】

また、第１の発明の通信システムは、好ましくは、前記通信装置は、前記サービス提供装置との間で、当該サービス提供装置が提供するサービスあるいは商品を受けるための所定の情報の送受信を行う。

【００２１】

また、第１の発明の通信システムは、好ましくは、前記サービス提供装置は、前記サービスあるいは商品に関しての支払い手続を行う旨の指示を前記通信装置

から受けると、当該サービスあるいは商品についての前記支払い請求情報を前記通信装置に送信し、前記通信装置は、前記サービス提供装置から受信した支払い請求情報の内容を表示あるいは出力し、当該内容に同意したことを示す指示をユーザから受けた後に、前記支払い請求情報を前記管理装置に送信する。

【００２２】

また、第１の発明の通信システムは、好ましくは、前記管理装置は、前記共通鍵を保持し、前記支払い処理情報の生成、並びに前記共通鍵を用いた暗号化を行う第１の管理装置と、前記第１の管理装置から入力した前記暗号化された前記支払い処理情報について当該管理装置の秘密鍵を用いて前記署名情報を作成し、前記暗号化された支払い処理情報と前記署名情報とを前記通信装置に送信する第２の管理装置とを有する。

【００２３】

また、第１の発明の通信システムは、好ましくは、前記通信装置および前記管理装置は、前記通信装置と前記管理装置との間で情報または要求を送受信する際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において当該秘密鍵に対応する公開鍵を用いて検証する。

【００２４】

また、第１の発明の通信システムは、好ましくは、前記通信装置および前記サービス提供装置は、前記通信装置と前記サービス提供装置との間で情報または要求を送受信する際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において当該秘密鍵に対応する公開鍵を用いて検証する。

【００２５】

また、第１の発明の通信システムは、好ましくは、前記通信装置、前記サービス提供装置および前記管理装置は、ネットワークを介して前記情報の送受信を行う。

【００２６】

また、第２の発明の通信装置は、サービス提供装置が提供するサービスあるいは商品に対しての支払い処理をＩＣカードを用いて行う場合に、当該ＩＣカードとの間で情報の入出力を行う他の通信装置および管理装置との間で通信を行う通

信装置であって、前記ＩＣカード内で支払い処理を行うための支払い処理情報を当該通信装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し、当該暗号化した支払い処理情報の正当性を示す当該通信装置の署名情報を生成し、前記暗号化した支払い処理情報と前記署名情報とを前記他の通信装置に送信する。

【００２７】

第２の発明の通信装置の作用は以下のようになる。

先ず、前記ＩＣカード内で支払い処理を行うための支払い処理情報を当該通信装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化する。

次に、当該暗号化した支払い処理情報の正当性を示す当該通信装置の署名情報を生成する。

次に、前記暗号化した支払い処理情報と前記署名情報とを前記他の通信装置に送信する。

【００２８】

また、第２の発明の通信装置は、好ましくは、当該通信装置の秘密鍵を用いて前記署名情報を作成する。

【００２９】

また、第２の発明の通信装置は、好ましくは、前記サービス提供装置が作成した前記署名情報の正当性を、前記サービス提供装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記支払い処理情報と前記管理装置の前記署名情報とを前記他の通信装置に送信する。

【００３０】

また、第２の発明の通信装置は、好ましくは、前記共通鍵を保持し、前記支払い処理情報の生成、並びに前記共通鍵を用いた暗号化を行う第１の管理装置と、前記第１の管理装置から入力した前記暗号化された前記支払い処理情報について当該通信装置の秘密鍵を用いて前記署名情報を作成し、前記暗号化された支払い処理情報と前記署名情報とを前記他の通信装置に送信する第２の管理装置とを有する。

【００３１】

また、第３の発明の通信方法は、前記管理装置において、前記ＩＣカード内で支払い処理を行うための支払い処理情報を前記サービス提供装置からの情報に基づいて生成し、当該支払い処理情報を当該管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し、当該暗号化した支払い処理情報と当該管理装置の署名情報とを前記管理装置から前記通信装置に送信し、前記通信装置において、前記管理装置から受信した前記署名情報の正当性を検証した後に、前記支払い処理情報を前記ＩＣカードに出力する。

【００３２】

また、第３の発明の通信方法は、前記管理装置において、当該管理装置の秘密鍵を用いて前記署名情報を作成し、前記通信装置において、前記秘密鍵に対応する公開鍵を用いて前記署名情報の正当性を検証する。

【００３３】

また、第３の発明の通信方法は、前記サービス提供装置において、前記支払い請求情報の正当性を示す署名情報を当該サービス提供装置の秘密鍵を用いて作成し、当該署名情報が付された前記支払い請求情報を、前記通信装置を介して前記サービス提供装置から前記管理装置に送信し、前記管理装置において、前記サービス提供装置が作成した前記署名情報の正当性を、前記サービス提供装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記支払い処理情報と前記管理装置の前記署名情報とを前記通信装置に送信する。

【００３４】

また、第３の発明の通信方法は、好ましくは、前記通信装置は、前記ＩＣカードにアクセス可能なアクセス装置との間で、前記支払い処理情報の出力、並びに所定の情報の入出力を行う。

【００３５】

また、第３の発明の通信方法は、好ましくは、前記ＩＣカードは、耐タンパ性のモジュール内で、前記支払い処理情報に応じた前記支払い処理を行う

【００３６】

【発明の実施の形態】

以下、本発明の実施形態に係わるネットワークシステムについて説明する。

図１は、本実施形態のネットワークシステム１の全体構成図である。

図１に示すように、ネットワークシステム１は、ユーザ２、決済機関３および店舗４の間でネットワーク５を介した通信を行う。

〔ユーザ２〕

ユーザ２には、ＩＣカード２０にアクセスを行うためのＲ／Ｗ装置２１およびパーソナルコンピュータ２２が設けられている。

ここで、ＩＣカード２０が第１～３の発明のＩＣカードに対応し、パーソナルコンピュータ２２が第１および第３の発明の通信装置、第２の発明の他の通信装置に対応している。また、ＩＣカードＲ／Ｗ装置２１が本発明のアクセス装置に対応している。

【００３７】

ＩＣカード２０は、図２（Ａ）に示すように耐タンパ性のＩＣモジュール５０を有し、図２（Ｂ）に示すように当該ＩＣモジュール５０内に処理回路５１およびメモリ５２を内蔵している。

処理回路５１は、共通鍵を用いた復号処理、所定の情報および要求に応じた処理、並びに相互認証処理などの種々の処理を行う。

メモリ５２は、決済機関３のセキュリティサーバ３１との間で共用する共通鍵K_Cを記憶している。

ＩＣカード２０は、図３に示すように、ＩＣカードＲ／Ｗ装置２１、インターフェースプログラム２４、ブラウザプログラム２３、パーソナルコンピュータ２２、ネットワーク５およびアプリケーションサーバ３０を介して、セキュリティサーバ３１との間で送受信する情報を、共通鍵K_Cを用いた共通鍵暗号方式によって暗号化および復号する。

【００３８】

ＩＣカードＲ／Ｗ装置２１は、ＩＣカード２０のＩＣモジュール５０との間で非接触方式あるいは接触方式でデータ入出力を行うと共に、パーソナルコンピュ

ータ２２との間との間で情報および要求の入出力を行う。

【００３９】

パーソナルコンピュータ２２は、ユーザによるキーボードやマウスなどの操作に応じて、ブラウザプログラム２３を実行すると共に、ブラウザプログラム２３上で、後述するようにネットワーク５を介して決済機関３のアプリケーションサーバ３０から受信したインターフェースプログラム２４を実行する。

パーソナルコンピュータ２２は、ディスプレイ、キーボードおよびマウスなどを有している。

ここで、インターフェースプログラム２４が第１および第３の発明のインターフェースプログラムに対応している。

【００４０】

ブラウザプログラム２３は、図４に示すように、パーソナルコンピュータ２２上で動作するプログラムであり、店舗４のネットワークサーバ４０のＨＴＴＰＳレイヤ６０との間で、ＰＫＩプロトコルにより、送信元において自らの秘密鍵を用いた署名情報の付加、並びに送信先において当該秘密鍵に対応する公開鍵を用いた当該署名情報の検証を行う。

【００４１】

インターフェースプログラム２４は、図５に示すように、パーソナルコンピュータ２２上で動作し、決済機関３のアプリケーションサーバ３０のＡＰＳ上位レイヤ３０ａとの間で、ＰＫＩプロトコルにより、送信元において自らの秘密鍵を用いた署名情報の付加、並びに送信先において当該秘密鍵に対応する公開鍵を用いた当該署名情報の検証を行う。

また、インターフェースプログラム２４は、ブラウザプログラム２３を実行中に、Ｒ／Ｗ装置２１を介してＩＣカード２０などのローカル資源へのアクセスを容易に実現するための機能拡張プログラムである。

【００４２】

〔決済機関３〕

決済機関３には、アプリケーションサーバ３０、セキュリティサーバ３１および情報管理サーバ３２が設けられている。

ここで、アプリケーションサーバ３０、セキュリティサーバ３１および情報管理サーバ３２が、第１および第３の発明の管理装置および第２の発明の通信装置に対応している。

また、セキュリティサーバ３１が本発明の第１の管理装置に対応し、アプリケーションサーバ３０が本発明の第２の管理装置に対応している。

アプリケーションサーバ３０は、ネットワーク５を介して、パーソナルコンピュータ２２およびネットワークサーバ４０と通信が可能である。

また、アプリケーションサーバ３０は、店舗４のネットワークサーバ４０の秘密鍵$K_{SHOP,S}$に対応した公開鍵$K_{SHOP,P}$を保持し、後述するように、ネットワークサーバ４０が生成した金額情報ＢＩＬＬに付された署名情報ＳＩＧを検証する。

また、アプリケーションサーバ３０は、図５に示すように、ＡＰＳ上位レイヤ３０ａおよびＡＰＳ下位レイヤ３０ｂを有する。

【００４３】

セキュリティサーバ３１は、ユーザ２のＩＣカード２０との間で共用する共通鍵K_Cを記憶している。

セキュリティサーバ３１は、図３に示すように、ＩＣカードＲ／Ｗ装置２１、インターフェースプログラム２４、ブラウザプログラム２３、パーソナルコンピュータ２２、ネットワーク５およびアプリケーションサーバ３０を介して、ＩＣカード２０との間で送受信する情報を、共通鍵K_Cを用いた共通鍵暗号方式によって暗号化および復号する。

【００４４】

情報管理サーバ３２は、例えば、登録されたユーザの個人情報を記憶および管理する。

【００４５】

〔店舗４〕

店舗４には、ネットワークサーバ４０が設けられている。

ここで、ネットワークサーバ４０が本発明のサービス提供装置に対応している。

ネットワークサーバ４０は、図４に示すように、パーソナルコンピュータ２２上で動作するブラウザプログラム２３との間で、パーソナルコンピュータ２２上で動作するプログラムである。

また、ネットワークサーバ４０は、例えば、商品あるいはサービスの紹介情報を記憶すると共に、店舗４がユーザ２に請求する金額を示す請求額情報ＢＩＬＬ（本発明の支払い請求情報）と、当該請求額情報に対して自らの秘密鍵$K_{SHOP,S}$を用いて作成した署名情報ＳＩＧとを生成する。

【００４６】

以下、図１に示すネットワークシステム１の動作を説明する。

図６は、ネットワークシステム１の動作を説明するための図である。

先ず、図６に示すユーザによる商品決定が行われる前に、ユーザ２がパーソナルコンピュータ２２上で動作するブラウザプログラム２３を用いて、ネットワーク５を介して、店舗４のネットワークサーバ４０にアクセスを行う。当該アクセスにより、ネットワーク５を介してネットワークサーバ４０からパーソナルコンピュータ２２に、店舗４が提供する商品情報が送信され、それに応じた画面がパーソナルコンピュータ２２のディスプレイに表示される。

【００４７】

以下、ネットワークシステム１の動作を図６～図８に示す各ステップ毎に説明する。

なお、以下に示す動作において、パーソナルコンピュータ２２とネットワークサーバ４０との間で情報あるいは要求の送受信を行う際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において、当該秘密鍵に対応する公開鍵を用いて検証するが、当該処理については記載を省略する。

また、同様に、パーソナルコンピュータ２２とアプリケーションサーバ３０との間で情報あるいは要求の送受信を行う際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において、当該秘密鍵に対応する公開鍵を用いて検証するが、当該処理についてはステップＳＴ１４，ＳＴ１５を除いて記載を省略する。

【００４８】

ステップＳＴ１：

パーソナルコンピュータ２２とネットワークサーバ４０との間でＳＳＬ(Secure Socket Layer）を用いた相互認証を行い、セキュアな通信路を確立する。

ステップＳＴ２：

ユーザ２が、パーソナルコンピュータ２２のキーボードやマウスなどを操作して購入を希望する商品を決定すると、それに応じた商品決定情報がパーソナルコンピュータ２２からネットワークサーバ４０に送信される。

ステップＳＴ３：

ネットワークサーバ４０は、パーソナルコンピュータ２２から商品決定情報を受けると、その見積もり情報をパーソナルコンピュータ２２に送信する。

ステップＳＴ４：

パーソナルコンピュータ２２は、ネットワークサーバ４０から受けた見積もり情報をディスプレイに表示する。ユーザ２は、当該見積もりに同意した場合には、パーソナルコンピュータ２２のキーボードなどを操作して請求額要求をネットワークサーバ４０に出す。

【００４９】

ステップＳＴ５：

ネットワークサーバ４０は、パーソナルコンピュータ２２から請求額要求を受けると、店舗４がユーザ２に請求する金額を示す請求額情報ＢＩＬＬと、当該請求額情報ＢＩＬＬに対して自らの秘密鍵$K_{SHOP,S}$を用いて作成した署名情報ＳＩＧと、インターフェースプログラム２４とをパーソナルコンピュータ２２に送信する。

ステップＳＴ６：

パーソナルコンピュータ２２は、ステップＳＴ５でネットワークサーバ４０から受信した請求額情報ＢＩＬＬが示す金額をディスプレイに表示する。

【００５０】

ステップＳＴ７：

ステップＳＴ６でディスプレイに表示された金額に同意したユーザ２がパーソナルコンピュータ２２のキーボードなどを用いて所定の指示を出すと、ステップＳＴ５でネットワークサーバ４０から受信したインターフェースプログラム２４

が起動される。

そして、パーソナルコンピュータ２２は、起動されたインターフェースプログラム２４を用いて、決済機関３のアプリケーションサーバ３０との間でＳＳＬを用いた相互認証を行い、セキュアな通信路を確立する。

【００５１】

ステップＳＴ８：

パーソナルコンピュータ２２は、ステップＳＴ５で店舗４のネットワークサーバ４０から受信した請求額情報ＢＩＬＬと、当該請求額情報に対しての署名情報ＳＩＧとを含む決済要求を決済機関３のアプリケーションサーバ３０に送信する。

ステップＳＴ９：

アプリケーションサーバ３０は、例えば、情報管理サーバ３２から読み出した店舗４に対応する公開鍵$K_{SHOP,P}$を用いて、ステップＳＴ８で受信した署名情報ＳＩＧを検証し、当該署名情報ＳＩＧが店舗４のネットワークサーバ４０において付された正当なものであると判断すると、ステップＳＴ１０の処理を行う。

なお、アプリケーションサーバ３０は、署名情報ＳＩＧが不正なものであると判断した場合には、例えば、パーソナルコンピュータ２２に対してのその旨を通知した後、処理を終了する。

【００５２】

ステップＳＴ１０：

アプリケーションサーバ３０は、例えば、請求額情報ＢＩＬＬを含む決済要求をセキュリティサーバ３１に送信する。

ステップＳＴ１１：

セキュリティサーバ３１は、ＩＣカード２０から決済要求を受けると、ＩＣカード２０との間で相互認証を行い、ＩＣカード２０との間で用いる共通鍵K_Cからセッション鍵K_{SES}を生成する。

また、ＩＣカード２０でも、同様に、共通鍵K_Cからセッション鍵K_{SES}を生成する。

【００５３】

ステップＳＴ１２：

セキュリティサーバ３１は、残高読み出し要求ＢＲＣ（本発明の残高情報読み出し要求）を生成し、これをセッション鍵K_{SES}で暗号化してアプリケーションサーバ３０に出力する。

アプリケーションサーバ３０は、セキュリティサーバ３１から入力した残高読み出し要求ＢＲＣを、パーソナルコンピュータ２２に送信する。

パーソナルコンピュータ２２は、アプリケーションサーバ３０から受信した残高読み出し要求ＢＲＣを、ＩＣカードＲ／Ｗ装置２１を介してＩＣカード２０に出力する。

【００５４】

ステップＳＴ１３：

ＩＣカード２０は、パーソナルコンピュータ２２からの残高読み出し要求ＢＲＣを入力すると、これをステップＳＴ１１で生成したセッション鍵K_{SES}を用いて復号する。

そして、ＩＣカード２０は、残高読み出し要求ＢＲＣに応じた処理回路５１の処理によって、ＩＣカード２０内の耐タンパ性のメモリ５２から残高情報ＢＩ（本発明の残高情報）を読み出し、これをセッション鍵K_{SES}を用いて暗号化した後に、パーソナルコンピュータ２２に出力する。

パーソナルコンピュータ２２は、ＩＣカード２０からの残高情報ＢＩを、アプリケーションサーバ３０に送信する。

アプリケーションサーバ３０は、パーソナルコンピュータ２２から受信した残高情報ＢＩを、セキュリティサーバ３１に出力する。

セキュリティサーバ３１は、アプリケーションサーバ３０から入力した残高情報ＢＩをセッション鍵K_{SES}を用いて復号し、ログ情報（本発明の履歴情報）を生成する。

【００５５】

ステップＳＴ１４：

セキュリティサーバ３１は、ステップＳＴ１３で生成したログ情報をＩＣカー

ド２０に書き込むためのログ書き込み情報と、ＩＣカード２０に記憶された残高情報が示す金額から請求額を減算するための減算額を示す減算情報とを含む決済処理要求ＳＰＣ（本発明の支払い処理情報）を生成し、これをセッション鍵K_{SES}を用て暗号化する。

次に、セキュリティサーバ３１は、平文の残高情報ＢＩと、暗号化された決済処理要求ＳＰＣとをアプリケーションサーバ３０に出力する。

アプリケーションサーバ３０は、セキュリティサーバ３１から入力した残高情報ＢＩおよび決済処理要求ＳＰＣに対しての署名情報SIG_{APL}を、アプリケーションサーバ３０の秘密鍵を用いて作成する。

次に、アプリケーションサーバ３０は、セキュリティサーバ３１から入力した残高情報ＢＩおよび決済処理要求ＳＰＣと、署名情報SIG_{APL}とをパーソナルコンピュータ２２に送信する。

【００５６】

ステップＳＴ１５：

パーソナルコンピュータ２２は、アプリケーションサーバ３０から受信した署名情報SIG_{APL}の正当性を、アプリケーションサーバ３０の公開鍵を用いて検証し、その正当性が認められた後に以下に示す処理を行う。パーソナルコンピュータ２２は、アプリケーションサーバ３０から受信した残高情報ＢＩが示す残高、並びにステップＳＴ３でネットワークサーバ４０から受信した見積もり情報が示す金額（請求額）をディスプレイに表示する。

ステップＳＴ１６：

パーソナルコンピュータ２２は、ステップＳＴ１５でディスプレイに表示された残高および請求額に同意したユーザ２がパーソナルコンピュータ２２のキーボードなどを用いて所定の指示を出すと、決済処理要求ＳＰＣをＩＣカードＲ／Ｗ装置２１を介してＩＣカード２０に出力する。

【００５７】

ステップＳＴ１７：

ＩＣカード２０は、パーソナルコンピュータ２２から入力した決済処理要求ＳＰＣをセッション鍵K_{SES}を用いて復号し、当該決済処理要求に応じた決済処理

を処理回路５１で実行する。

具体的には、ＩＣカード２０は、処理回路５１の処理によって、決済処理要求ＳＰＣに含まれるログ書き込み情報を、ＩＣカード２０内の耐タンパ性のメモリ５２に記憶する。また、ＩＣカード２０は、処理回路５１の処理によって、メモリ５２に記憶されている残高情報が示す残高から、決済処理要求ＳＰＣに含まれる減算情報が示す減算額を減算し、その結果を残高情報としてメモリ５２に記憶する。

【００５８】

ステップＳＴ１８：

ＩＣカード２０は、ステップＳＴ１７の処理が完了すると、処理が完了したことを示す処理完了通知ＰＣＮ（本発明の支払い完了通知）を生成し、これをセッション鍵K_{SES}で暗号化した後に、パーソナルコンピュータ２２およびアプリケーションサーバ３０を介して、セキュリティサーバ３１に送信する。

ステップＳＴ１９：

セキュリティサーバ３１は、ＩＣカード２０からの処理完了通知ＰＣＮを受信すると、これをセッション鍵K_{SES}を用いて復号し、処理完了通知ＰＣＮを確認した後に、決済完了通知ＡＣＮを生成し、これをアプリケーションサーバ３０を介してパーソナルコンピュータ２２およびネットワークサーバ４０に送信する。

ステップＳＴ２０：

パーソナルコンピュータ２２は、セキュリティサーバ３１からの決済完了通知ＡＣＮを受信すると、これに応じた情報をディスプレイに表示する。

【００５９】

以上説明したように、ネットワークシステム１によれば、ＩＣカード２０のメモリ５２に共通鍵K_Cを記憶し、秘密鍵は記憶しない。そのため、ユーザ２がＩＣカード２０を紛失した場合でも、メモリ５２には秘密鍵が記憶されていないため、秘密鍵を用いてユーザ２の署名が不正に行われることを回避できる。

【００６０】

また、ネットワークシステム１によれば、共通鍵K_CはＩＣカード２０およびセキュリティサーバ３１の内部でのみ使用されることから、共通鍵K_Cが盗まれ

る危険性を低くでき、安全な取り引きを実現できると共に、鍵管理を容易にすることができる。

【００６１】

また、ネットワークシステム１によれば、ＩＣカード２０に入出力される情報および要求をパーソナルコンピュータ２２を介して行い、パーソナルコンピュータ２２と、アプリケーションサーバ３０およびネットワークサーバ４０との間で情報および要求を送受信する際に、秘密鍵および公開鍵を用いた署名検証を行うことから、当該情報および要求がネットワーク５上で不正に改竄されることを回避でき、ネットワーク５を用いた取り引きの安全性を確保できる。

【００６２】

また、ネットワークシステム１によれば、店舗４のネットワークサーバ４０において、請求額情報ＢＩＬＬに対して自らの秘密鍵$K_{SHOP,S}$を用いて作成した署名情報ＳＩＧを付し、決済機関３のアプリケーションサーバ３０において、秘密鍵$K_{SHOP,S}$に対応する公開鍵$K_{SHOP,P}$を用いて署名情報ＳＩＧを検証し、当該署名情報ＳＩＧが店舗４のネットワークサーバ４０において付された正当なものであると判断することから、ユーザ２のパーソナルコンピュータ２２などにおいて、不正に改竄された請求額情報ＢＩＬＬに基づいて決済が行われてしまうことを防止できる。

【００６３】

また、ネットワークシステム１では、前述したように、パーソナルコンピュータ２２は、アプリケーションサーバ３０から受信した残高情報ＢＩが示す残高、並びにネットワークサーバ４０から受信した見積もり情報が示す金額（請求額）をディスプレイに表示し、その内容にユーザ２が同意した後に、アプリケーションサーバ３０から受信した決済処理要求ＳＰＣをＩＣカードＲ／Ｗ装置２１を介してＩＣカード２０に出力する。従って、ユーザ２は、ＩＣカード２０内で最終的に行われる決済処理の内容を事前に確認でき、不正に改竄された内容で決済処理が行われることを防止できる。

また、ネットワークシステム１によれば、決済処理に伴う手順を従来に比べて少なくでき、ネットワーク５を介した情報伝送を削減でき、ネットワーク５の利

用量の削減、並びに処理時間を短縮を図れる。

また、ネットワークシステム１によれば、従来のＳＥＴ方式のように、署名情報の作成および検証を多数回行う必要がない。

【００６４】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、図１に示すように、決済機関３において、アプリケーションサーバ３０、セキュリティサーバ３１および情報管理サーバ３２を別々に設けた場合を例示したが、これらのサーバの機能を一つのサーバで実現してもよい。

また、上述した実施形態では、ＩＣカード２０内の残高情報をアプリケーションサーバ３０に読み出す場合を例示したが、当該残高情報をアプリケーションサーバ３０に読み出さないようにしてもよい。

【００６５】

【発明の効果】

以上説明したように、本発明によれば、共通鍵を保持したＩＣカードを用いて、ネットワークを介した電子商取引を安全に行う通信システム、通信装置および通信方法を提供できる。

【図面の簡単な説明】

【図１】

図１は、本発明の実施形態のネットワークシステムの全体構成図である。

【図２】

図２は図１に示すＩＣカードを説明するための図である。

【図３】

図３は、ユーザのＩＣカードと、決済機関のセキュリティサーバとの間の通信方法を説明するための図である。

【図４】

図４は、ユーザのパーソナルコンピュータと、店舗のネットワークサーバとの間の通信方法を説明するための図である。

【図５】

図５は、ユーザのパーソナルコンピュータと、決済機関のアプリケーションサーバとの間の通信方法を説明するための図である。

【図６】

図６は、図１に示すネットワークシステムの動作を説明するための図である。

【図７】

図７は、図１に示すネットワークシステムの動作を説明するための図である。

【図８】

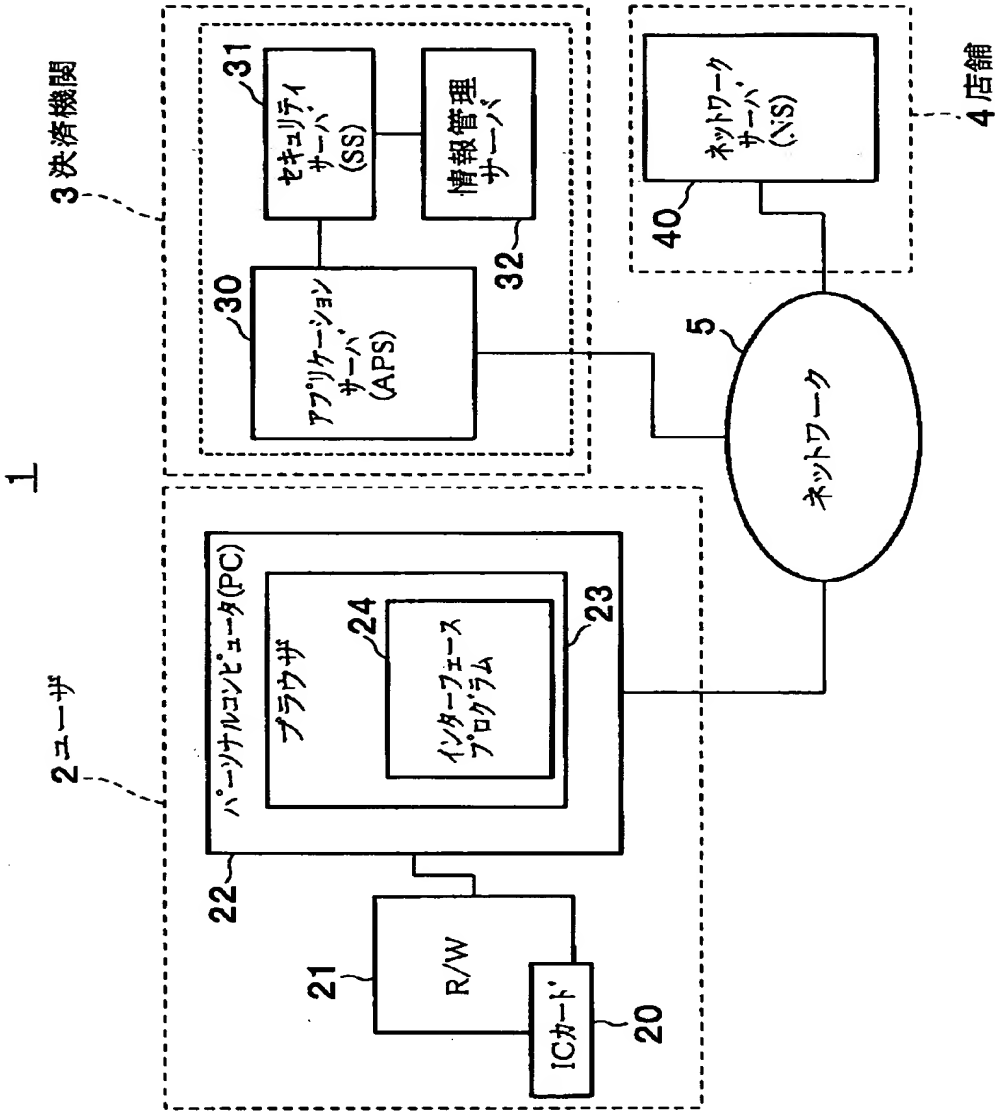
図８は、図１に示すネットワークシステムの動作を説明するための図である。

【符号の説明】

１…ネットワークシステム、２…ユーザ、３…決済機関、４…店舗、５…ネットワーク、２０…ＩＣカード、２１…ＩＣカードＲ／Ｗ装置、２２…パーソナルコンピュータ、２３…ブラウザプログラム、２４…インターフェースプログラム、３０…アプリケーションサーバ、３１…セキュリティサーバ、３２…情報管理サーバ、４０…ネットワークサーバ

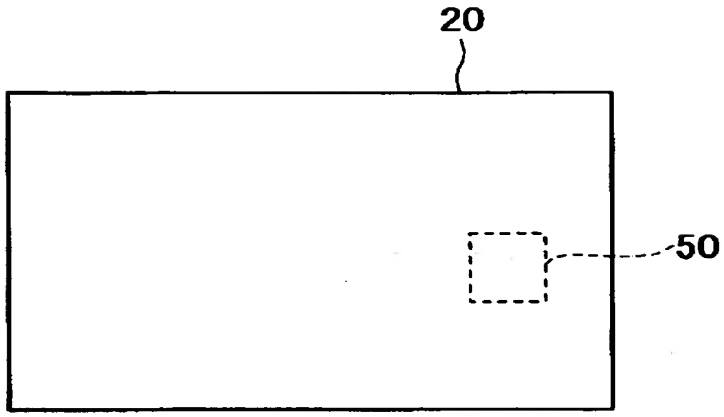
【書類名】　図面

【図１】

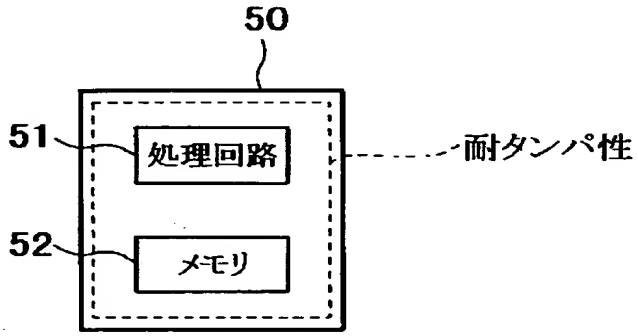

1
2ユーザ
3決済機関
4店舗
5
ネットワーク
パーソナルコンピュータ(PC)
ブラウザ
インターフェース プログラム
23
24
22
R/W
21
ICカード
20
アプリケーション サーバ (APS)
30
セキュリティ サーバ (SS)
31
情報管理 サーバ
32
ネットワーク サーバ (NS)
40

【図２】

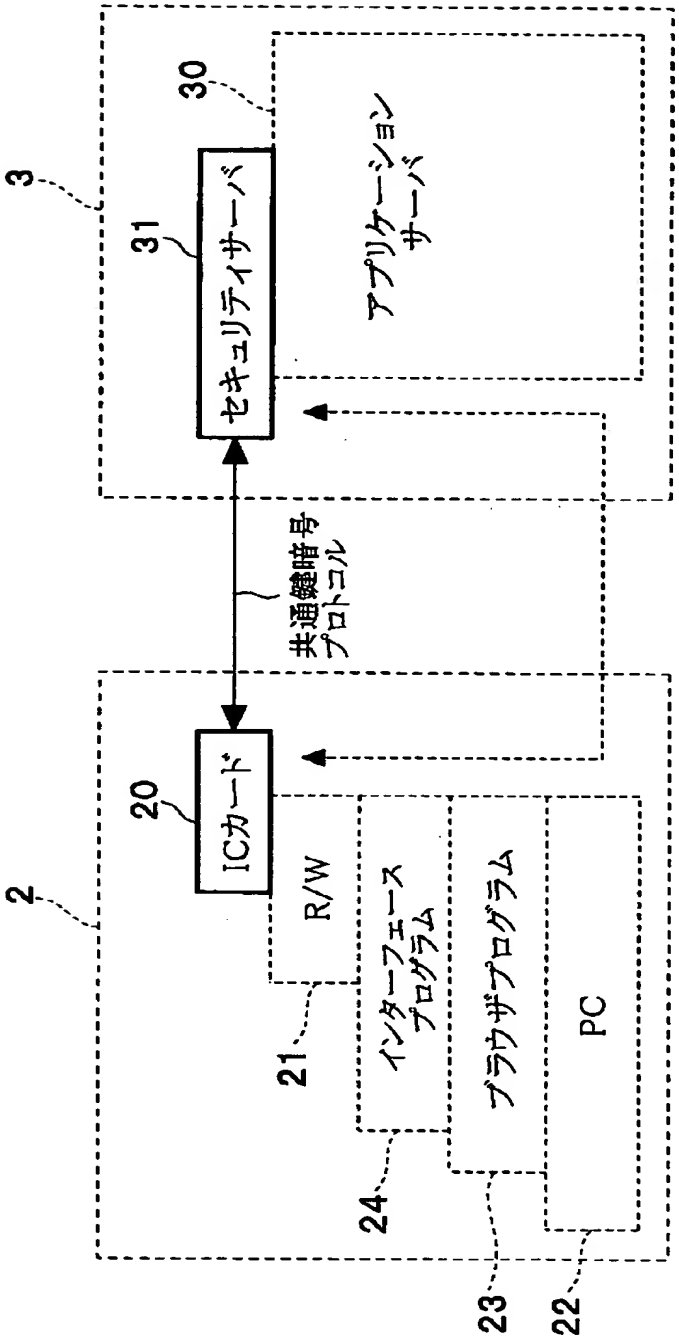
(A)



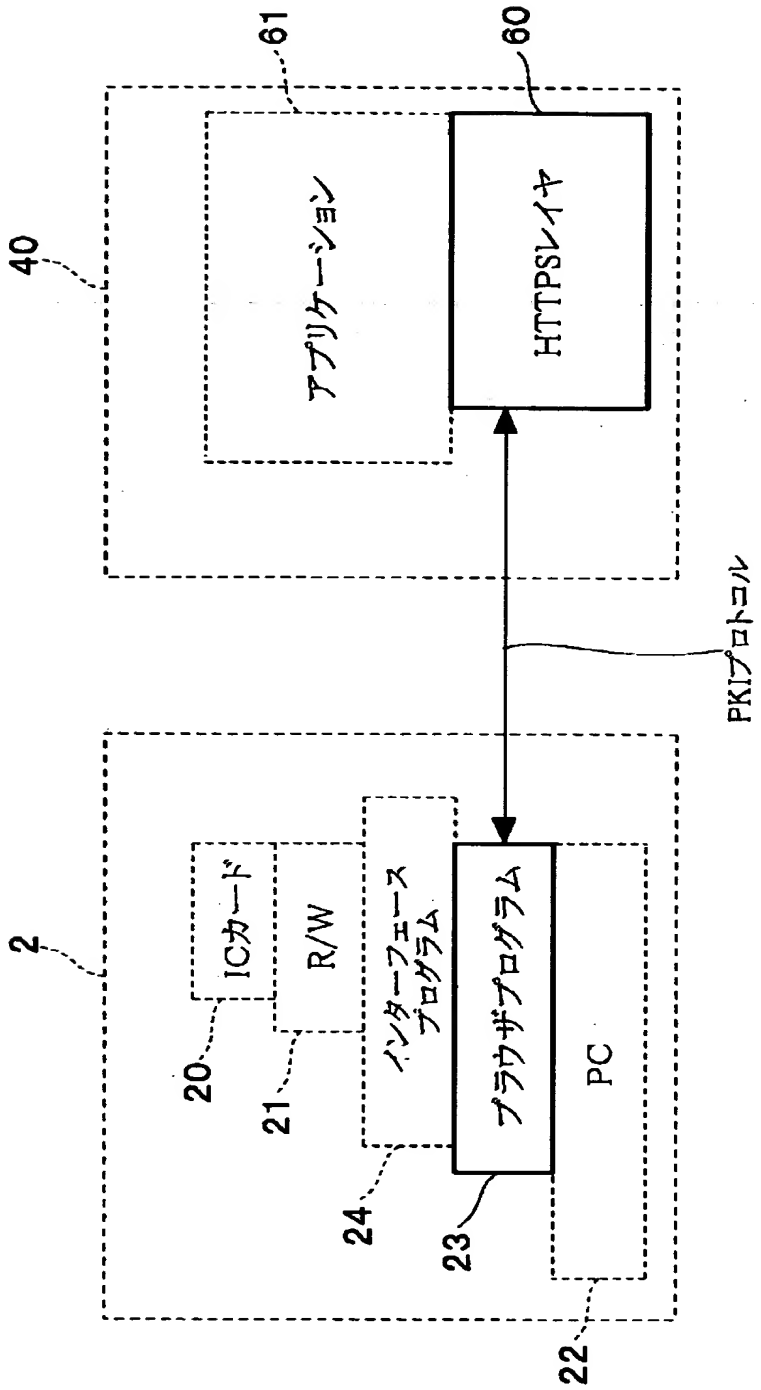
(B)



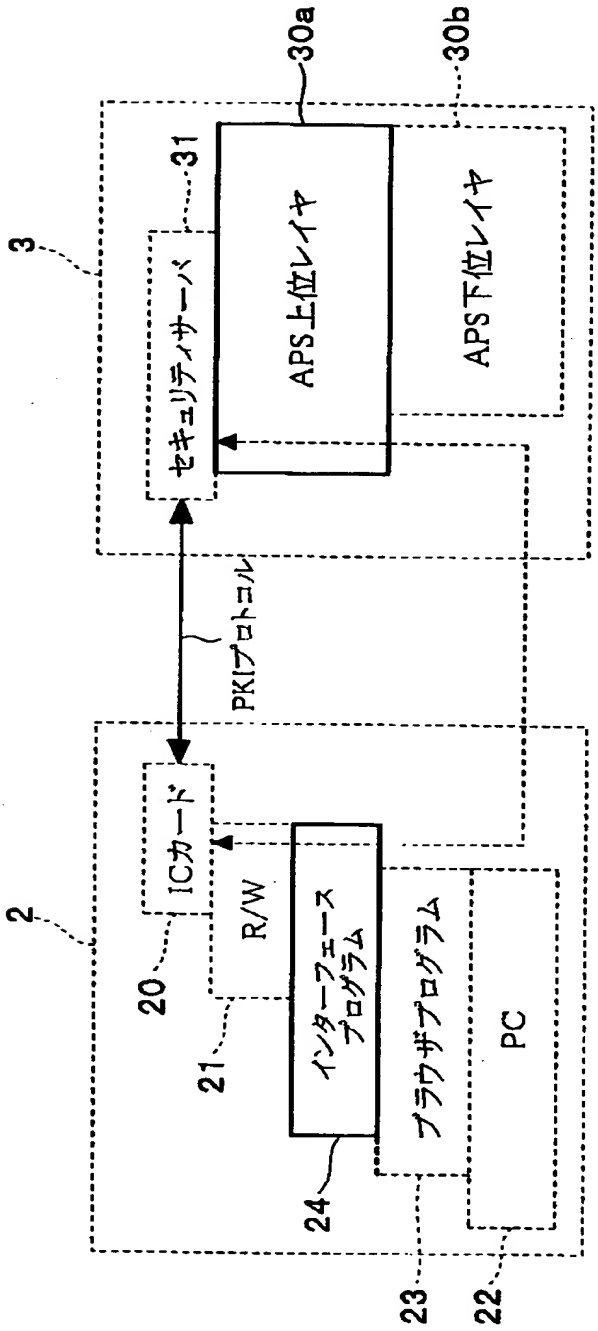
【図３】


3
30
アプリケーション
サーバ
31
セキュリティサーバ
共通鍵暗号
プロトコル
2
20
ICカード
R/W
21
インターフェース
プログラム
24
ブラウザプログラム
23
PC
22

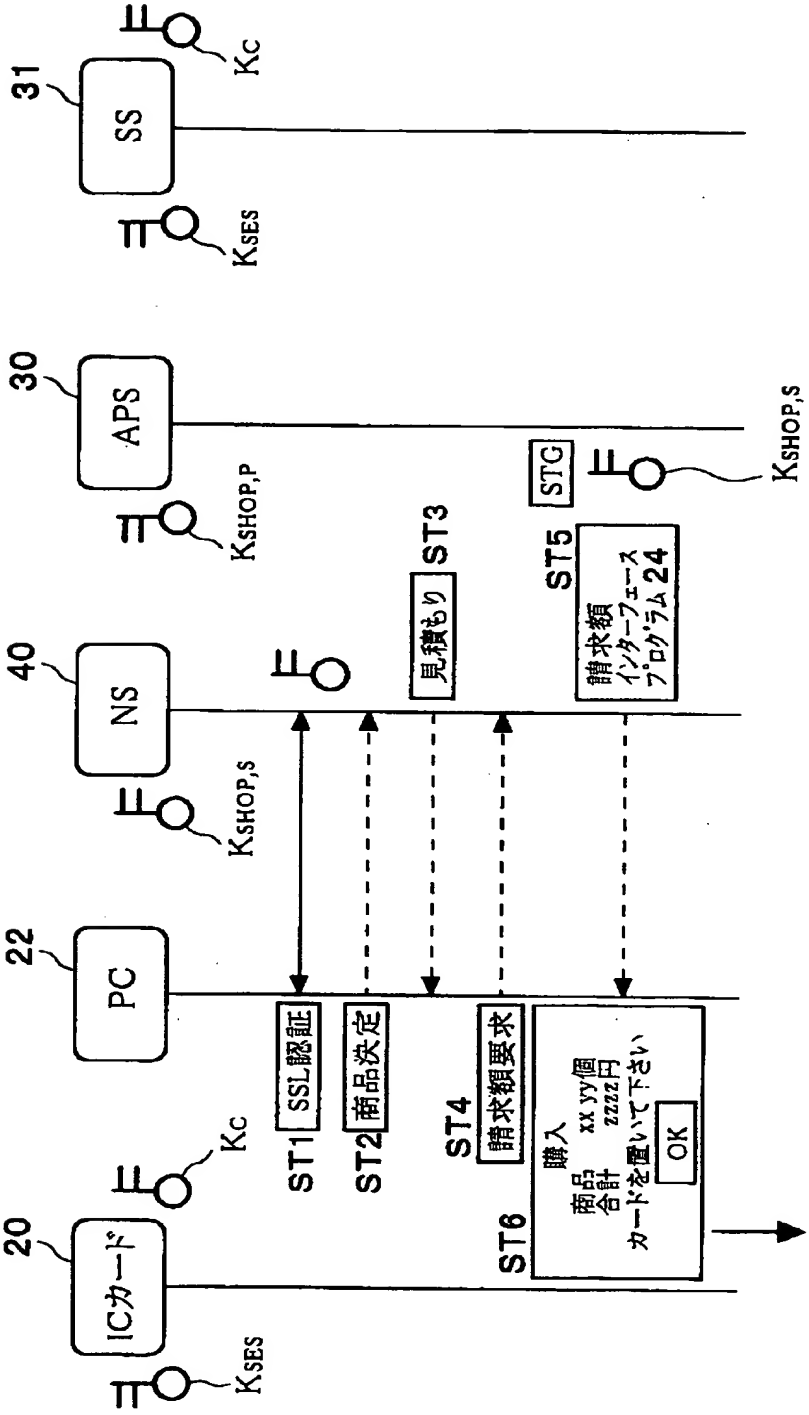
【図４】


61
60
アプリケーション
HTTPSレイヤ
40
PKIプロトコル
2
ICカード
R/W
インターフェース
プログラム
ブラウザプログラム
PC
20
21
24
23
22

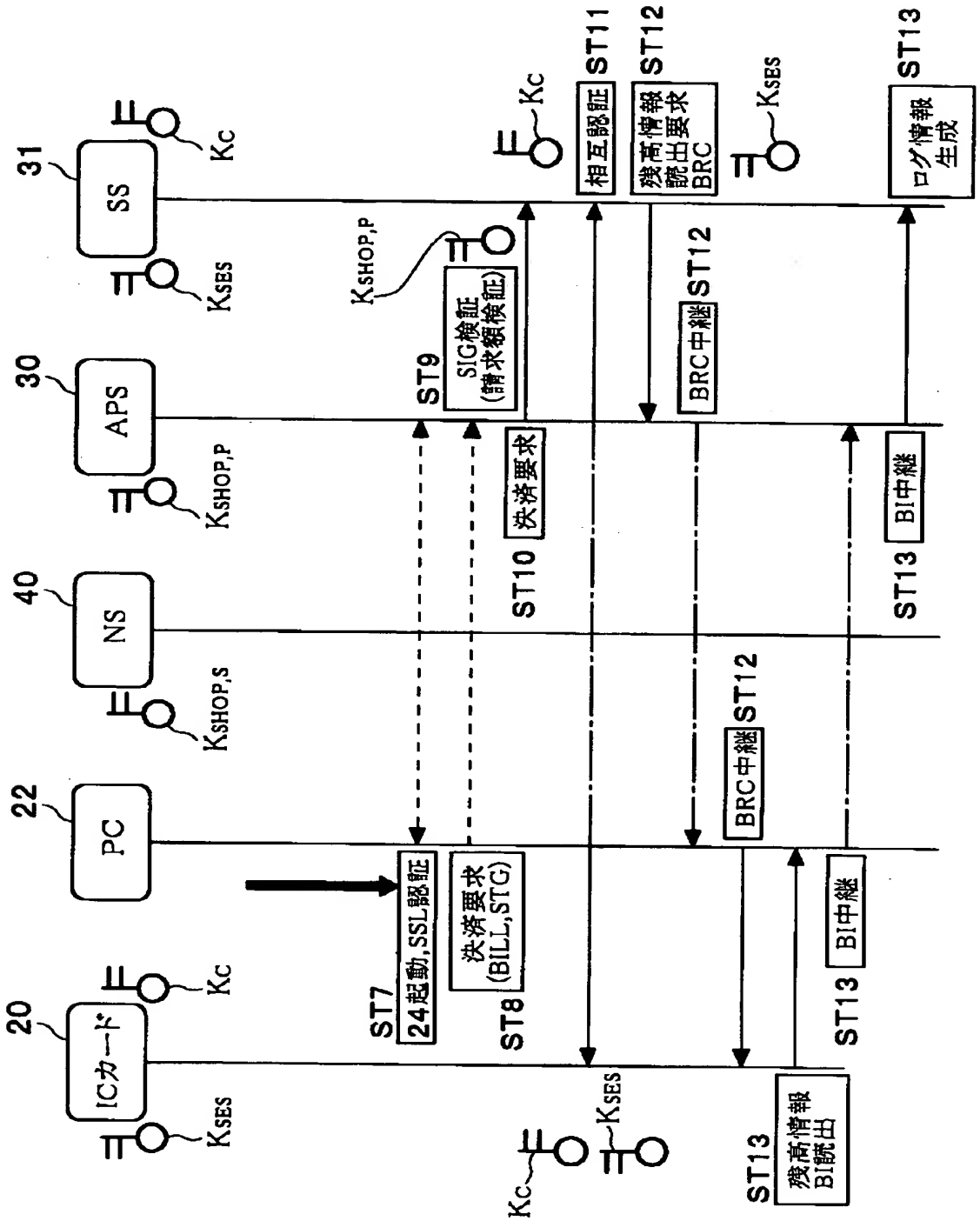
【図５】


30a
30b
31
3
セキュリティサーバ
APS上位レイヤ
APS下位レイヤ
PKIプロトコル
ICカード
R/W
インターフェース
プログラム
ブラウザプログラム
PC
2
20
21
24
23
22

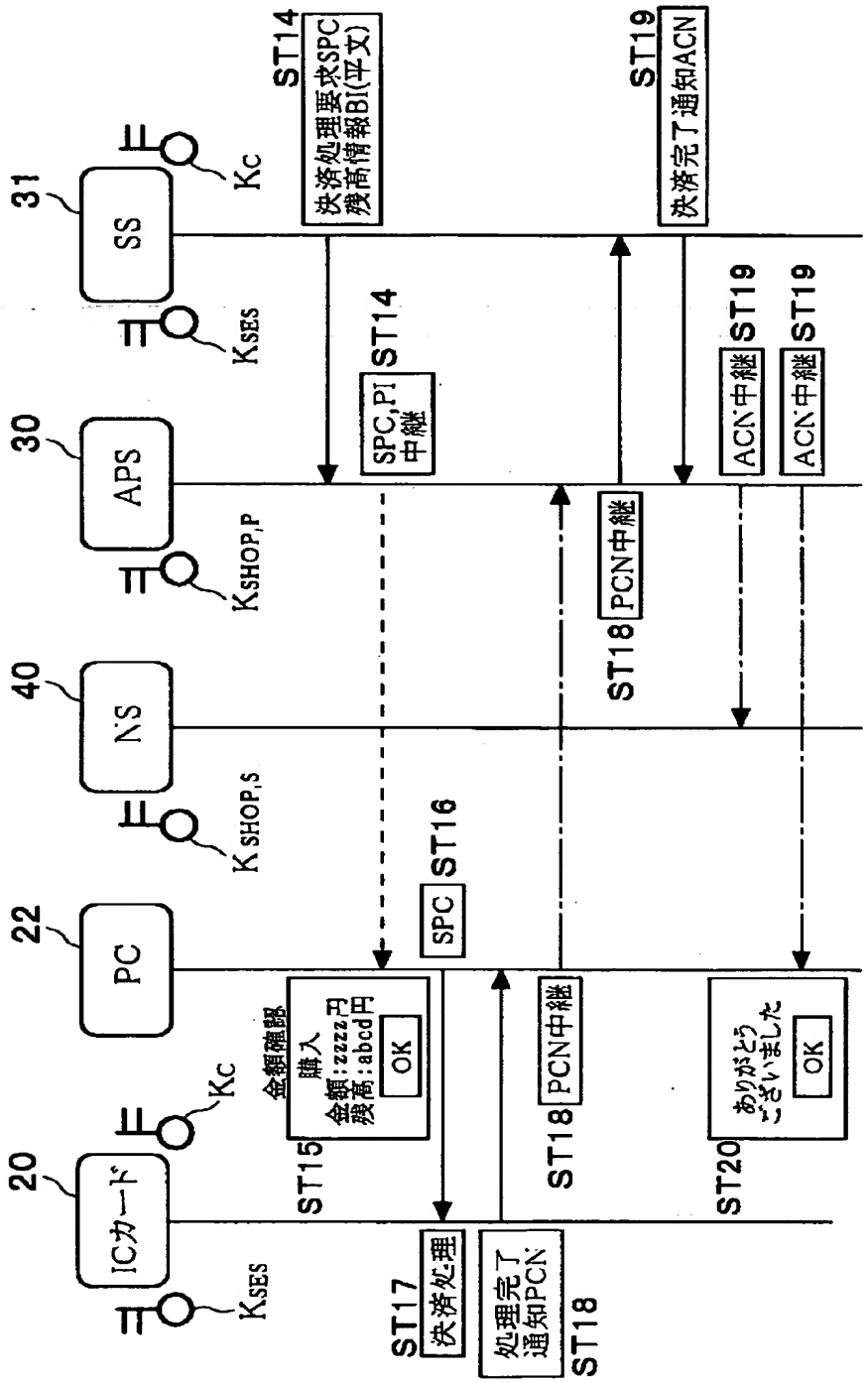
【図６】


31
SS
Kc
KSES
30
APS
KSHOP,P
KSHOP,S
STG
ST5
請求額
インターフェース
プログラム24
ST3
見積もり
40
NS
KSHOP,S
22
PC
ST1
SSL認証
ST2
商品決定
ST4
請求額要求
ST6
購入
xx yy個
商品
zzzz円
合計
カードを置いて下さい
OK
Kc
20
ICカード
KSES

【図７】


20
ICカード
22
PC
40
NS
30
APS
31
SS
Kc
KSES
KSHOP,S
KSHOP,P
KSBS
ST7
24起動,SSL認証
ST8
決済要求
(BILL,STG)
ST9
SIG検証
(請求額検証)
ST10
決済要求
ST11
相互認証
ST12
残高情報
読出要求
BRC
BRC中継
ST13
BI中継
ログ情報
生成
残高情報
BI読出

【図８】


31
SS
Kc
KSES
30
APS
KSHOP,P
40
NS
KSHOP,S
22
PC
Kc
20
ICカード
KSES
ST14
決済処理要求SPC
残高情報BI(平文)
SPC,PI
中継
ST14
PCN中継
ST18
SPC
ST16
金額確認
購入
金額:zzzz円
残高:abcd円
OK
ST15
PCN中継
ST18
ST17
決済処理
処理完了
通知PCN
ST18
ST19
決済完了通知ACN
ACN中継
ST19
ACN中継
ST19
ありがとう
ございました
OK
ST20

【書類名】　　要約書

【要約】

【課題】　共通鍵を保持したＩＣカードを用いて、ネットワークを介した電子商取引を安全に行うことができる通信システムを提供する。

【解決手段】　アプリケーションサーバ３０において、ネットワークサーバ４０において生成された請求額情報の正当性が署名情報を用いて判断される。その後、セキュリティサーバ３１において、決済処理要求が、ＩＣカード２０との間の共通鍵K_Cを用いて暗号化された後に、アプリケーションサーバ３０において署名情報を付してパーソナルコンピュータ２２に送信される。パーソナルコンピュータ２２では、署名情報を検証後に、決済処理要求をＩＣカード２０に出力する。決済処理要求は、ＩＣカード２０において共通鍵K_Cを用いて復号された後に実行される。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
　［変更理由］　新規登録
　　住　所　　東京都品川区北品川６丁目７番３５号
　　氏　名　　ソニー株式会社